答弁書

特許庁審査官　殿

1．国際出願の表示　　ＰＣＴ／ＪＰ９８／００３４２

2．出願人

名称　　トヨタ自動車株式会社
TOYOTA JIDOSHA KABUSHIKI KAISHA

あて名　〒471-0826　日本国愛知県豊田市トヨタ町１番地
1, Toyota-cho, Toyota-shi, Aichi-ken 471-0826, JAPAN

国籍　　日本国　JAPAN

住所　　日本国　JAPAN

3．代理人

氏名　　７９０４　弁理士　　中島　淳
NAKAJIMA Jun

あて名　〒160-0022　日本国東京都新宿区新宿４丁目３番１７号
ＨＫ新宿ビル７階　太陽国際特許事務所
ＴＡＩＹＯ，　ＮＡＫＡＪＩＭＡ　＆　ＫＡＴＯ
Seventh Floor, HK-Shinjuku Bldg., 3-17,
Shinjuku 4-chome, Shinjuku-ku, Tokyo 160-0022, JAPAN

4．通知の日付

１８．０８．９８

5．答弁の内容

（１）１９９８年８月１８日（発送日）付けの見解書によれば、請求項１乃至請求項７は、文献１（ＪＰ，８－７１３９，Ａ）により進歩性なしとされています。

そこで、その見解書に鑑み、本書と同日付けで手続補正書を提出して明細書を補正し、以下に答弁致します。なお、請求の範囲の補正について概説すれば、請求項１乃至請求項７を削除し、本発明の要旨を明確にしております。

（２）請求項８について、

文献１では、自動課金システムの路車間及びカードの各々の間での情報授受において暗号鍵により暗号化した暗号データを用いて情報授受させる技術が開示されています。具体的には、自動料金収受のため、精算情報等を格納した記憶媒体に対して書き込む情報に暗号鍵により暗号化した暗号データを用いることによって、セキュリティ機能を強化して、不正使用やデータ改ざんに対する確実な対処を可能としています。　しかしながら、文献１では、１つの暗号鍵を用いることによって、セキュリティ機能を強化していますが、暗号鍵により暗号化した暗号データを用いる場合には、同一の暗号鍵を用いていたのでは、その暗号データが授受される回数に応じて秘匿性が失われることになります。すなわち、同一の暗号鍵が流通することになるので、暗号データによりセキュリティ機能が強化はされているものの外部に触れてその暗号鍵が漏洩することが増加します。このため、暗号鍵の秘匿性が損なわれやすくなり、秘匿性が損なわれたときにはシステム全体のセキュリティ機能が低下します。

これに対して本願発明は複数の暗号鍵を用いることができます。すなわち、自動課金システムでは、例えば路側と車側との間、車両内ではＩＣカードと通信機との間等のように、情報授受に複数の段階や種類があります。このため、同一の暗号鍵を流通させた場合、何れの段階や何れの種類でも外部に触れることが可能となり、暗号鍵の秘匿性が損なわれやすくなります。本願発明では、１システム内における情報授受において複数の暗号鍵を用いることができるので、それぞれの段階での情報は異なる暗号鍵により漏洩が困難となります。

このように、情報通信及び情報授受に異なる暗号鍵を用いて独立した秘匿性を有させているので、路車間通信装置として安全性を向上でき、また、独立した秘匿性を有させているので、秘匿性が明らかになるまでを最小限に抑えることができます。これらの点は、文献１には、考慮はなく、示唆もありません。

従って、文献１に記載の技術から、秘匿性が明らかになるまでを最小限に抑えることができることを案出することは到底できないと判断されます。

このように、請求項８については、文献１によって進歩性を有しないものではありません。

（３）請求項９について

請求項８が進歩性を有する限り当然に進歩性を有するものと考えます。

（４）明細書の補正は、補正された請求の内容に合致させるためのものであります。

以上

Response to Written Opinion

5. Contents of Response

(1) According to the Written Opinion dated August 18, 1998 (mailing date), claims 1 to 7 are each deemed to lack non-obviousness in light of document 1 (JP, 8-7139, A).

In light of the Written Opinion, we submit an Amendment, which is of the same date as this document, to amend the specification, and we respond as follows. To summarize the amendments to the claims, we have canceled claims 1 to 7 in order to clarify the subject matter of the present invention.

(2) Regarding claim 8

Document 1 discloses a technique wherein information is transferred between a road side and a vehicle side of an automatic accounting system and between each side and a card by using encryption data encrypted by a cipher key. Concretely, in order to collect a toll automatically, encryption data encrypted by a cipher key is used for information to be written in a storage medium in which settlement information and the like is stored, so as to strengthen a security function, and as a result, irregular usage or alteration of data can be prevented reliably. However, although in document 1 the security function is strengthened by using one cipher key, when using the encryption data encrypted by the cipher key, if the same cipher key is used, the security of the encryption data may be lost depending on the number of times of the

encryption data being transferred. Namely, since the same cipher key is circulated, the number of cases in which the cipher key leaks out due to being exposed to the outside increases, irrespective of the security function being strengthened by the encryption data. For this reason, the secrecy of the cipher key is likely to be impaired, and when the secrecy is impaired, the security function of an entire system deteriorates.

On the other hand, in the present invention, a plurality of cipher keys can be used. Namely, in the automatic accounting system, a plurality of steps and types for the transfer of information are provided, for example, the transfer thereof between the road side and the vehicle side, or in a vehicle interior, between an IC card and a communication machine. For this reason, when the same cipher key is circulated, any step or type allows the cipher key to be exposed to the outside and the secrecy of the cipher key is thereby likely to be impaired. In the present invention, a plurality of cipher keys can be used in the transfer of information within one system, and therefore, at each step, leakage of information becomes difficult, due to different cipher keys.

As described above, secrecy is independently maintained using different cipher keys for communication of information and transfer of information, and therefore, the security of a road-to-vehicle communication device can be improved. Further, since secrecy is maintained independently, leakage of the secrecy can be

restrained to the minimum. These points are neither disclosed nor suggested by document 1.

Accordingly, it is determined that, from the description given by document 1, it is impossible to conceive directly of being able to restrain leakage of the secrecy to the minimum until secrecy becomes obvious.

Thus, claim 8 does not lack non-obviousness in light of document 1.

(3) Regarding claim 9

Provided that claim 8 is non-obvious, claim 9 is also non-obvious as a matter of course.

(4) The amendments to the specification were made in order to have the specification correspond to the contents of the amended claims.

Response to Written Opinion

5. Contents of Response

(1) According to the Written Opinion dated August 18, 1998 (mailing date), claims 1 to 7 are each deemed to lack non-obviousness in light of document 1 (JP, 8-7139, A).

In light of the Written Opinion, we submit an Amendment, which is of the same date as this document, to amend the specification, and we respond as follows. To summarize the amendments to the claims, we have canceled claims 1 to 7 in order to clarify the subject matter of the present invention.

(2) Regarding claim 8

Document 1 discloses a technique wherein information is transferred between a road side and a vehicle side of an automatic accounting system and between each side and a card by using encryption data encrypted by a cipher key. Concretely, in order to collect a toll automatically, encryption data encrypted by a cipher key is used for information to be written in a storage medium in which settlement information and the like is stored, so as to strengthen a security function, and as a result, irregular usage or alteration of data can be prevented reliably. However, although in document 1 the security function is strengthened by using one cipher key, when using the encryption data encrypted by the cipher key, if the same cipher key is used, the security of the encryption data may be lost depending on the number of times of the

encryption data being transferred. Namely, since the same cipher key is circulated, the number of cases in which the cipher key leaks out due to being exposed to the outside increases, irrespective of the security function being strengthened by the encryption data. For this reason, the secrecy of the cipher key is likely to be impaired, and when the secrecy is impaired, the security function of an entire system deteriorates.

On the other hand, in the present invention, a plurality of cipher keys can be used. Namely, in the automatic accounting system, a plurality of steps and types for the transfer of information are provided, for example, the transfer thereof between the road side and the vehicle side, or in a vehicle interior, between an IC card and a communication machine. For this reason, when the same cipher key is circulated, any step or type allows the cipher key to be exposed to the outside and the secrecy of the cipher key is thereby likely to be impaired. In the present invention, a plurality of cipher keys can be used in the transfer of information within one system, and therefore, at each step, leakage of information becomes difficult, due to different cipher keys.

As described above, secrecy is independently maintained using different cipher keys for communication of information and transfer of information, and therefore, the security of a road-to-vehicle communication device can be improved. Further, since secrecy is maintained independently, leakage of the secrecy can be

restrained to the minimum. These points are neither disclosed nor suggested by document 1.

Accordingly, it is determined that, from the description given by document 1, it is impossible to conceive directly of being able to restrain leakage of the secrecy to the minimum until secrecy becomes obvious.

Thus, claim 8 does not lack non-obviousness in light of document 1.

(3) Regarding claim 9

Provided that claim 8 is non-obvious, claim 9 is also non-obvious as a matter of course.

(4) The amendments to the specification were made in order to have the specification correspond to the contents of the amended claims.